移动群智感知中支持隐私保护的动态激励机制 *

梁　艳[1,2]，安　健[2†]，胡先智[3]，司海峰[1]

(1. 西安思源学院 理工学院，西安 710038; 2. 西安交通大学深圳研究院，广东 深圳 518057; 3. 西安理工大学 网络信息管理中心，西安 710048)

摘　要：针对移动群智感知中高质量感知数据与参与用户隐私之间的矛盾，提出一种支持隐私保护的动态激励机制。首先，采用轻量级隐私保护方法，利用安全加密哈希函数为竞标用户生成不少于256位的可变地址序列，并结合随机数对候选用户节点的效用报价进行隐匿和约束；其次，通过定义区域热度、时间热度、数据完整率和数据质量等多维参数，实现任务价值与用户效用报价的动态平衡；最后，依据用户提交的效用报价和任务预算，并利用逆向拍卖思想，完成对任务参与节点的最优选择和动态激励。在群智感知系统模拟平台上进行仿真实验，结果表明所提机制不仅增强了隐私保护度和数据精确度，同时提升了时间效率和激励效果。

关键词：移动群智感知；隐私保护；激励机制；逆向拍卖；效用报价

中图分类号：TP309.2　　doi: 10.3969/j.issn.1001-3695.2018.07.0431

Dynamic incentive mechanism with privacy-preserving in mobile crowd sensing

Liang Yan[1, 2], An Jian[2†], Hu Xianzhi[3], Si Haifeng[1]

(1. *School of Technology*, *Xi'an Siyuan University*, *Xi'an* 710038, *China*; 2. *Shenzhen Research Institute of Xi'an Jiaotong University*, *Shenzhen Guangdong* 518057, *China*; 3. *Center of Network Information & Management*, *Xi'an University of Technology*, *Xi'an* 710048, *China*)

Abstract: Aiming at the contradiction between high-quality perception data and user privacy in mobile crowd sensing system, this paper proposed a dynamic incentive mechanism with privacy-preserving. Firstly, it used the lightweight privacy-preserving method and a secure encryption hash function to generate a variable address sequence of not less than 256 bits for the bidding user, and integrated a random number to conceal and constraint the data utility price of the candidate user node. Secondly, by defining multi-dimensional parameters such as regional heat, time heat, data integrity rate and data quality, it realized the dynamic balance between task value and data utility price. Finally, based on the data utility price of the user and task budget, and using the reverse auction, it completed the optimal selection and dynamic incentive for the task participation nodes. Simulation experiments on the mobile crowd sensing system simulation platform show that the proposed mechanism not only enhances the privacy-preserving and data accuracy, but also improves the time efficiency and incentive effect.

Key words: mobile crowd sensing; privacy-preserving; incentive mechanism; reverse auction; data utility price

0　引言

近年来，随着移动互联网、传感网络、社交网络的快速发展，移动群智感知（mobile crowd sensing, MCS）成为普适计算领域的前沿研究问题[1]。移动群智感知[2]是以普通用户的移动终端设备作为基本感知单元，通过移动互联网进行有意识或无意识的协作，实现感知任务分发与感知数据收集，完成大规模复杂的社会感知任务。移动群智感知应用依赖大量普通用户参与，而用户在参与感知时会消耗自身设备的电量、计算、存储、通信等资源并且存在个人隐私泄露的风险[3]。而隐私泄漏又是阻碍用户参与感知的一个重要因素。因此，设计合理的激励机制并能够有效保护用户个人隐私，对促进移动群智感知系统平台的长期稳定发展具有重要意义。

目前研究人员对群智感知各阶段的隐私保护问题做了许多研究，如分组统计，位置混淆，*k*-匿名，差分隐私等，但这些解决方案通常是引入注册机构/可信第三方或聚合服务器，以实

收稿日期：2018-07-13；**修回日期：**2018-09-10　**基金项目：**国家自然科学基金资助项目（61502380）；深圳市科技计划项目（JCYJ20170816100939373）；西安思源学院科研项目（XASY-B1802）

作者简介：梁艳（1980-），女，河南灵宝人，讲师，硕士，主要研究方向为移动群智感知；安健（1983-），男（通信作者），山西晋中人，高级工程师，硕导，博士，主要研究方向为群智感知、物联网安全及应用（anjian@mail.xjtu.edu.cn）；胡先智（1978-），男，湖北武人，工程师，硕士，主要研究方向为网络信息安全；司海峰（1977-），男，河北张家口人，讲师/工程师，硕士，主要研究方向为计算机网络安全.

现对感知数据、用户或用户位置的隐私保护。然而，大多数没有考虑竞标参与者报价隐私的泄露。因此，本文希望在更一般的环境中通过保护参与者的身份和报价隐私来补充现有的隐私方案，以实现更好的匿名性和隐私保护。

本文提出一种支持隐私保护的动态激励机制，利用安全加密哈希函数为竞标参与者生成不少于 256 位的可变地址序列作为注册编号，以此标识参与者竞标身份，实现匿名参与，并结合随机数对参与者的效用报价进行隐匿和约束，实现竞标中效用报价的隐私保护。效用报价由参与者的数据完整率、数据质量以及理想报价等多维参数确定。平台根据效用报价和任务预算对参与节点进行最优选择并支付，对竞标失败者按照任务预算剩余额度给予一定补偿。机制采用轻量级隐私保护方法和数据加密技术，结合合理的报酬支付方式，实现其激励作用。

1　相关工作

针对群智感知激励方式问题，近几年逐渐涌现出许多有价值的研究。现行的报酬支付激励是基于博弈论的方法，以微支付形式回报参与者的感知数据，是目前最常用的激励方式，其中逆向拍卖模型应用较广。文献[4]首次将经济领域中的逆向拍卖应用在群智感知激励机制研究中，在最小化支付代价的同时保证较高的参与率。该文提出逆向拍卖动态价格-虚拟参与积分机制(RADP-VPC)，选取参与者中报价最低的作为胜出者并支付，同时引入虚拟参与积分的概念，避免在竞标中屡次失败的参与者退出。文献[5]在 RADP-VPC 的基础上提出了基于位置的激励模型，在固定预算约束下选择区域覆盖率最大的参与者集合，但是以用户为中心的区域覆盖并不能适应用户位置的动态可变性和多样性。文献[6]采用逆向拍卖中的多属性拍卖机制，不仅考虑参与率问题，还考虑感知数据质量问题。服务器平台能够通过拍卖过程影响数据质量，同时，参与者能够通过拍卖结果的反馈提高自身感知数据的质量，从而提高竞标价格。然而，以上这些激励机制都不考虑参与者的隐私保护。

针对群智感知隐私保护问题，学者们研究了多种隐私保护技术，主要分为四类：分组统计、第三方验证、K-匿名、数字加密。文献[7]提出了 PriSense 隐私保护方案，过程包括切分重组和二分查找两部分，它能够支持各种非增量型数据聚集和快速获取聚集值，并对参与者的隐私保护强度和能耗进行均衡处理。文献[8]利用可信第三方为参与者提供匿名服务，参与者在可信第三方处注册自己的感知设备并安装参与感知的软件，验证通过后，可信第三方将参与者的个人信息映射到新用户空间，然后以新用户身份向服务器请求数据，参与者的数据传输由可信第三方负责。文献[9]提出一种连续 LBS(Location -based Service)请求下的需求感知位置隐私保护模型 DALP，通过删除最远足迹和缩小匿名区边界，最小化共同用户的历史足迹所形成的匿名区，以减小查询时延以及服务器的负载，来进一步提高用户请求服务质量。文献[10]采用基于身份加密的参与者数据隐私保护方法，它不依赖于传统公钥基础设施 PKI 和认证中心来向参与者绑定公钥，参与者的身份信息（如电话号码、身份证号码、邮件地址等）可以直接作为参与者的公钥，私钥则由受信任的私钥生成器 PKG 管理和颁发，该方法能为移动节点和请求者提供有效安全的通信。虽然这些隐私保护方案用不同技术对参与者的数据进行保护，但都没有考虑如何激励参与者提交高质量感知数据问题。为此，本文提出既支持参与者数据隐私保护又能激励参与者提交高质量感知数据的动态激励机制。

2　系统模型与问题分析

2.1　系统模型

本研究基于一个通用的移动群智感知系统，该系统包含三种角色，分别是：任务发布者，任务参与者（工作者或用户），拍卖基础设施。对这三种角色阐述如下。

a）任务发布者（task publisher）。对感知数据感兴趣或有一定需求的组织或个人，并对感知数据指定了时间有效期、位置或区域以及愿意为获得感知数据所希望支付的报酬等需求。

b）任务参与者（participant）。是使用智能手机等各种移动感知设备，按照任务发布者的需求进行感知数据采集的人员，也称工作者（task worker）或用户（user）。

c）拍卖基础设施（auction infrastructure）。由三种不同的服务器组成，它们同属于一个移动群智感知平台。三种服务器分别是任务服务器（task server,TS）、拍卖服务器（auction server,AS）和报表服务器（report server,RS）。任务服务器负责发布感知任务；拍卖服务器负责运行拍卖过程，此过程中参与者可以向拍卖服务器发起竞标；报表服务器负责收集胜出者（winner）的感知数据，并将数据转发给任务发布者。

图 1 描述了通用移动群智感知系统的三个工作阶段。首先，TS 发布来自任务发布者的感知任务（①），参与者的移动设备定期访问 TS，搜索是否有适合自身的任务并有选择性地下载（②）；然后，参与者按照任务发布者给出的任务属性等信息，到达目的地去完成感知任务（③），完成任务的工作者在拍卖阶段可以向 AS 进行注册并发起竞标，所提机制为参与者提供注册信息和效用报价的加密保护，以实现匿名参与（④），当拍卖结束后，AS 根据参与者的效用报价和发布者的任务预算选择胜出者（⑤）；最后，胜出者将感知数据提交给 RS（⑥），RS 验证后，AS 再将任务报酬支付给胜出者（⑦）。

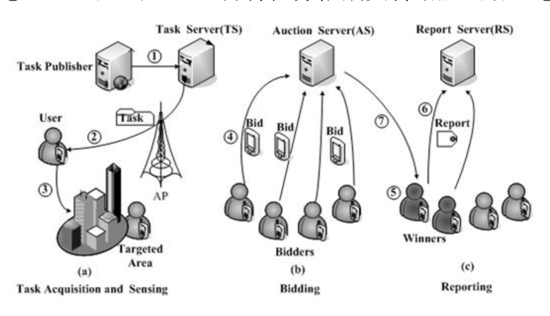


图 1　移动群智感知系统的工作流程

2.2　问题分析

2.2.1 隐私和公平需求

1）参与者的隐私

在竞标结束之前，参与者需要匿名，所有报价需要保秘，意味着参与者的身份信息不能以任何方式与其提交的报价联系在一起。这要求隐私保护措施要确保参与者在不泄露身份或设备标识的情况下完成竞标，其他人也不能推断有关参与者的任何信息。本文隐私保护方法采用安全加密哈希函数对参与者的身份和报价进行加密隐匿，和前人研究的重量级密码操作和原语（如秘密共享技术、多方计算、同态加密等）方案[11]不同，是一个轻量级且安全的方法，能支持参与者匿名参与。

2）公平和公正性

竞标过程中要求参与者不能根据其他人的竞标信息确定自己的报价，并且一旦提交效用报价，就不能否认或修改，以此保证竞标的公平性。竞标结束后进入开放阶段，竞标过程应经得起任何参与者验证，确保竞标的有效性和胜出者选择的公正性。因此，需要具有承诺措施，能够约束参与者的竞标行为，从而为所有参与者提供公平和公正的拍卖环境。方案包含承诺措施，通过哈希函数和随机数的使用可以确保参与者在竞标中对其效用报价的承诺。

2.2.2 胜出者选择和报酬支付

由于感知任务形式各异，加之采集环境的多变性，在缺少客观评价标准的情况下，任务发布者和参与者很难凭主观评估任务价值，可能导致发布者给出的任务预算难以让参与者满意，而参与者在竞标时也很难给出一个合理报价。因此，有必要设置一个能够客观评估任务价值的模块，为发布者和参与者提供参考依据。本机制为移动群智感知平台提供了任务价值评估策略，通过拍卖服务器在消息窗口发布任务价值，为任务发布者设置合适的任务预算和参与者设置合理报价提供参考。

选择胜出者时，如果仅考虑最低报价的参与者，可能导致参与者提交低质量的感知数据，不能满足任务发布者的需求。因此，平台在选择胜出者时，不能只关注报价，还要考虑参与者的数据质量，应对提供高质量数据且报价合理的参与者优先选择。因此，机制依据参与者的效用报价和发布者的任务预算来选择胜出者，而效用报价是由参与者的数据效用值（由数据完整率和数据质量决定）和参考任务价值后所提报价得出。为了保持较高的参与率，对竞标失败者也发放一定额度的报酬，将支付胜出者后的剩余预算平均分发给每个失败者，以此来避免在竞标中屡次失败的参与者退出。

3　支持隐私保护的动态激励方案设计

3.1　任务价值

在评估任务价值时，通过基于位置的社交网络 LBSN（location-based social networks）应用得到参与者签到数据[12]，利用该签到数据分析参与者的时空特性规律，再结合任务的时空特性计算任务价值。影响任务价值的评估有两个因素：区域热度和时间热度。区域热度是对任务所在区域中参与者访问频度的度量，时间热度是对任务有效时间内参与者访问频度的度量。这两个因素根据信息空间中参与者签到数据和物理空间中感知任务的时空特性计算得到。

区域热度 $L(O)$由分析 LBSN 线上数据中参与者对应的签到地点计算得出，如式(1)所示。

$$L(O)=\frac{\sum_{x\in U,j\in O}N_{x,j}}{\sum_{x\in U,j\in\tau}N_{x,j}}\times E(X)\tag{1}$$

$$E(X)=-\sum_{x_i\in X}(p(x_i)\times log_2 p(x_i))\tag{2}$$

其中：O 表示发布者指定的任务区域，$N_{x,j}$ 表示参与者 x 在地点 j 的签到次数，U 表示所有参与者的集合，τ表示所有签到地点的集合。式(1)中的 $E(X)$由式(2)计算得到。$E(X)$表示区域 O 中访问参与者的多样性，通过计算区域信息熵得到。X 表示在区域 O 签到的参与者集合，$X=\{x_1,x_2,\dots,x_n\}$。$p(x_i)$表示参与者 x_i 在区域 O 签到的概率，即参与者 x_i 在区域 O 签到次数占在所有区域签到次数的比值。

如果区域信息熵越大，则在该区域签到的参与者提供的信息量越大，即该区域签到的参与者多样性程度越高。将区域热度归一化到 0~1 之间，取值越大意味着该区域的访问人数越多，签到频率越高。

时间热度 $T(Z)$由分析 LBSN 线上数据中参与者的签到时间分布计算得出，取值在 0~1 之间，如式(3)所示。

$$T(Z)=\sum_{z\in Z}PV_z\tag{3}$$

$$PV_z=\frac{\sum_{x\in U,j\in O}N_{x,z,j}}{\sum_{x\in U,k\in A,j\in O}N_{x,k,j}}\tag{4}$$

由于参与者签到时间具有一定的弹性，为了任务评估的准确性，所以用一个小时为单位将一天分为 24 个时间段。式(4)中 A 表示 24 个时间段，$A=\{1,2,\cdots,24\}$。PV_z表示在第 z 个时间段内所有参与者访问区域 O 的概率。$N_{x,z,j}$表示参与者 x 在第 z 个时间段内访问地点 j 的次数。式(3)中 Z 表示任务覆盖的时间段集合，$Z\subseteq A$。

基于区域热度和时间热度，对于任意一个任务，可由式(5)计算得到任务价值 V。

$$V=\frac{LA}{L(O)}\times\frac{TA}{T(Z)}\tag{5}$$

LA 表示可由式(1)得到的参与者签到数据中所有区域矩形块的区域热度平均值，TA 表示可由式(3)、(4)得到的所有参与者签到的时间热度的平均值。定义当区域热度为 LA，时间热度为 TA 时任务价值为基准值 1，该基准值是任务的单位价值。式(5)表示任务价值与所在区域热度和时间热度成负相关。也就是说，对于一个任务，参与者采集数据的时间和区域热度越高，在该区域和该时间段的任务就越容易完成，相应该任务的价值就较低，反之，任务价值就越高。

一个任务的价值一旦被平台评估确定后，就及时公布于消息窗口，以便所有参与者参考，同时，也便于任务发布者对任务预算进行动态调整。

3.2 数据效用值

任务工作者的表现对数据质量有很大影响。本文用数据效用值作为数据质量的衡量指标。而数据质量测量基于两个主要因素：数据完整率和质量指标。

1）数据完整率（*CR*）

数据完整率定义为已完成任务量占所需完成任务总量的比值。*CR* 是对任务工作者完成任务量的度量。对于具有预定义点集合 *P* 的任务，可以对任务工作者所采集的感应点采用基于感应点与 *P* 中每个点的最短距离方式进行分组。如果最短距离超过阈值 *r*，则感应点将被视为与任务无关。否则，此感应点将被分组到 *P* 中的关联点。然后，可根据一个任务工作者的数据覆盖点数 *TWP* 来计算此工作者对于集合 *P* 的 *CR* 值，如式(6)所示。

$$CR_w = \frac{|TWP|}{|P|} \tag{6}$$

2）质量指标（*QI*）

衡量数据质量是一个较难的问题。本文仅讨论数字数据的质量测量。对于每个数据组 *G* 可以计算一个成员到其所在组中心的距离。对于每个数据，用 1 减去平均距离与其组的最大距离的比率来表示单个 *QI*，则一个任务工作者所有数据的平均值即为此工作者的数据质量指标 *QI*（$0 < QI \leq 1$），计算如式(7)所示。假设一个工作者的所有数据集合为 $D_w=\{d_1,d_2,\ldots,d_n\}$。

$$QI_w = \frac{\sum_{i=1}^{|D_w|}\left(1-\frac{d_i-G(d_i).center}{MaxDis(G(d_i))}\right)}{|D_w|} \tag{7}$$

3）数据效用值（*DU*）

基于数据的完整率 *CR* 和质量指标 *QI* 两个因素，可得出一个任务工作者的数据效用值 DU_w，如式(8)所示。

$$DU_w = CR_w \times QI_w \tag{8}$$

3.3 效用报价

参与者要想在竞标中获胜，需要给出合理报价，因此，需结合自身的数据效用值和平台给出的任务价值进行报价，才能保证较大胜出率。参与者参考平台任务价值 *V* 提出理想报价 *BV*，再计算出自身效用报价作为竞价。效用报价 BU_w 由式(9)计算得到。

$$BU_w = BV \times (1 - DU_w) \tag{9}$$

3.4 拍卖

拍卖过程包括三个主要阶段：注册、竞标和开放。在注册阶段，每个参与者进行匿名注册来保护自己的身份隐私。在竞标阶段，确保每个参与者的效用报价对于其他参与者不可见。在开放阶段，拍卖服务器公开每个参与者的效用报价，但仍保持参与者身份信息隐匿，拍卖服务器根据效用报价确定匿名胜出者。一旦胜出者上传了其感知数据，经报表服务器验证通过后，就会得到相应的报酬。

假定在拍卖服务器上存在用于服务器和参与者进行信息交换的“合约消息窗口”。一旦消息发布到消息窗口，任何参与者都可以阅读，但不能删除或更改。因此，合约消息窗口是一个广播程序模块，任何参与者都可以接收广播消息，而且消息可以被任何参与者验证。拍卖服务器的公钥 *k* 通过发布于消息窗口来告知每个参与者，参与者可以使用此公钥 *k* 将信息加密发送给拍卖服务器并验证由服务器签名的消息。用 *Hash*()表示一个具有不少于 256 位输出的安全加密哈希函数。“安全”意味着 *Hash*()是单向的和抗冲突的。因此，反转哈希函数或者寻找满足 *Hash*（*x*）=*Hash*（*y*）的 *x* 和 *y* 在计算上是不可行的。

3.4.1 注册

竞标开始之前拍卖服务器向消息窗口发布其公钥以及拍卖的各种参数，如拍卖 *ID*、拍卖各阶段开始/结束时间等。一旦注册开始，每个参与者在规定注册时间内，向 AS 发送一个匿名编号 *BidderID* 来标识其在竞标中的身份信息。*BidderID* 由参与者随机选取的一次性临时公钥k^e的哈希值 $Hash(k^e)$生成。AS 收到后将此信息发布到消息窗口，每个参与者就可以核实自己的 *BidderID* 对于本次竞标是否已被成功注册。

定义 1　如果（k，k^{-1}）是实体 *A* 的一对密钥，则 $Sig_{A,k^{-1}}(m)$ 表示实体 *A* 用私钥 k^{-1} 对信息 *m* 创建的数字签名，用σ表示，即$\sigma=Sig_{A,k^{-1}}(m)$。$Sig.verify_{A,k}(m, \sigma)$则表示用 *A* 的公钥 *k* 对信息 *m* 的数字签名σ解密验证的结果（真或假）。

算法 1. 参与者匿名注册（Anonymous Registration）

输入：参与者 *b* 的一次性临时公钥 k^e。

输出：参与者 *b* 的经过拍卖服务器 *A* 签名授权的匿名注册编号 *BidderID*。

1. h=Hash（k^e），h 是 b 的匿名注册编号 BidderID；
2. $h^*=r^{e_A}*h \bmod N_A$，r：新随机数，e_A：A 的公钥，N_A：加密算法模量，h^*：加密后的 BidderID；
3. b→A：h^* and　$\sigma=Sig_{b,k^{e-1}}(h^*)$；
4. if $Sig.verify_{b,k^e}(h^*, \sigma)$=true then
5. 　A→b：$\sigma^*=Sig_{A,,d_A}(h^*)$，$d_A$ 是 A 的私钥，
6. end if
7. $\sigma'=r^{-1}*\sigma^* \bmod N_A$，b 得到 A 关于 h 的数字签名$\sigma'$。

算法 1 不但支持参与者匿名注册，而且最终也为参与者生成了一个授权的临时公钥 k^e。在感知数据提交阶段只要参与者提供了这样的凭证，就被认为是授权用户。因此这种方式也是一种验证临时密钥的方法。

3.4.2 竞标

注册结束后进入竞标阶段，参与者用隐匿的效用报价进行竞标，而且必须遵守竞标承诺。承诺方案是在提交者和接收方之间执行一对算法（*Commit*，*Open*）。提交报价时，参与者执行算法 *Commit*，同时需要输入消息 *m* 和辅助信息 *rm*（一个不可预知的随机数）来产生一次提交 C_m=*Commit*(*m*，*rm*)。承诺方案应具有较强的约束力和隐匿性，确保接收方在开放阶段之前不能获得关于 *m* 的任何信息，也保证恶意提交者无法找到一组替代值（*m*′，*rm*′），能使开放算法 *Open*（C_m, *m*′, *rm*′）=*Open*（C_m, *m*, *rm*）。

本文隐私保护采用简单方法即哈希函数 *H*，为提交算法 *Commit* 生成承诺报价 CBU_w，如式(10)所示。

$$CBU_w = Commit(BU_w, r_w) = H(r_w||BU_w) \qquad (10)$$

其中：r_w 为用来隐匿 BU_w 的随机数。

参与者需向拍卖服务器发送一个用自身私钥 k^{-1} 签名的消息σ_b，如式(11)所示。

$$\sigma_b = Sig_{b,k^{-1}}(ActionID||BidderID'||CBU_w) \qquad (11)$$

其中，*ActionID* 为本次竞标编号，*BidderID'*为加密后参与者注册编号。

采用轻量级隐私保护方法既能确保竞价的隐匿，又能约束参与者不能随意否认或更改报价。此外，报价在消息窗口公布，以便任何参与者都可以验证其报价已被正确提交给拍卖服务器。当拍卖服务器接收到σ_b时，它能够确定是来自平台的合法参与者，因为是用带有其签名的公钥完成验证。因此，临时密钥充当授权凭证，允许服务器隐式验证参与者但却不能识别参与者。

3.4.3 开放

当拍卖服务器公告竞标结束时，每个参与者的效用报价 BU_w 真值就显现出来。在接收到 BU_w 和 r_w 后，拍卖服务器评估 $Commit(BU_w, r_w) = H(r_w||BU_w)$并继续使用与参与者相关联的临时密钥来验证签名$\sigma_b$。拍卖服务器对报价验证后，会根据任务预算选择前 n 个 BU_w 值最低的参与者作为胜出者。然后，在消息窗口广播一个已签名的消息，包含胜出者的匿名编号 *BidderID*、临时公钥以及效用报价 BU_w。因此，任何参与者都可以通过计算$H(r_w||BU_w)$来验证本次竞标的正确性，确保了拍卖过程的公平公正。

算法 2. 竞标—开放（Bidding-Opening）

输入：参与者 b 的效用报价 BU_w 和一个新随机数 r_w。

输出：拍卖服务器签名的 n 个胜出者节点消息。

竞标阶段

1. $Commit = H(r_w||BU_w)$，b 得到 CBU_w；
2. $b \rightarrow AS$：$\sigma_b = Sig_{b,k^{e-1}}(ActionID||BidderID'||CBU_w)$；

开放阶段

3. 初始化集合 $S=\emptyset$；
4. for b_i from b_1 to b_n do
5. 　$m_i=(ActionID||BidderID'||H(r_w||BU_w))$；
6. 　if $Sig.verify_{b,k^e}(m_i, \sigma_b)=true$ then
7. 　　$S=S+\{m_i\}$；
8. 　end if
9. end for
10. 对集合 S 按照 BU_w 值升序排序，得到新集合 S'，并将 S'内容发布于消息窗口；
11. 初始化：胜出者集合 $W=\emptyset$，　W 中当前节点个数 $n=0$，胜出者节点总数为 N；
12. $x=S'.FirstElement()$；
13. while $TotalB>0$ and $n<N$ do
14. 　$W=W+\{x\}$；
15. 　$n=n+1$；
16. 　$TotalB=TotalB-TotalB_x$；
17. 　$x=S'.NextElement()$；
18. end while
19. return W，胜出者节点发布于消息窗口，即

$AS \rightarrow *$: $Sig_{AS}(AuctionID,(BidderID_1, k_1^e, BU_{w1}, r_{w1}),\ldots)$。

3.5 支付措施

选出的胜出者可以向报表服务器传送感知数据，报表服务器对收到的数据进行验证，如果合格，便依据胜出者的效用报价对其进行支付。对所有上传了合格数据的胜出者支付完成后，若任务预算有剩余，则平均发放给竞标失败者，以此给失败者一定补偿。

4 性能分析

对方案从隐私保密性、正确性、不可否认性、不可链接性和激励有效性等方面进行性能分析。

1）隐私保密性

由于参与者注册时，采用安全加密哈希函数 *Hash*()对参与者的一次性临时公钥生成一个不少于 256 位的哈希值来标识参与者竞标身份，且 *Hash*()具有抗冲突性，能够确保任何参与者的注册编号唯一，因此，参与者的身份隐私信息能够被较好地保护。又因为效用报价以$H(r_w||BU_w)$形式在竞标中出现，哈希函数 H 的单向性和随机数 r_w 的使用能够确保效用报价保持隐匿且不能被其他参与者推断，同时也消除了合谋的可能性，因此方案对于参与者的竞价具备隐私保密性。

2）正确性

由于竞标结束后所有参与者的效用报价 BU_w和所用随机数 r_w 都公布于消息窗口，所以任何参与者都可以验证竞标的正确性。因此，不可能有假报价出现或已发生的报价被改变（由于散列函数 H 的抗碰撞性），能够保证竞标的正确性和公正性。

3）不可否认性

由于每一次报价都携带着参与者的数字签名，并且哈希函数的抗冲突性能确保不可能找到一个（r'，BU'）集合，使得 H（$r'||BU'$）$=H$（$r||BU$），所以一旦开始竞标，参与者就不能否认或修改其报价。此外，如果竞标出现争议，竞标承诺可用于解决争议，承诺值（r，BU）和参与者的数字签名可用于证明竞标的真实性。所以，能够对参与者的竞标行为进行很好地约束。

4）竞标的不可链接性

此属性与参与者身份隐私有关。为确保不能将同一参与者在不同竞标中提交的两个报价联系起来，因此，本方案支持参与者每次竞标采用不同的匿名编号和公钥，保证了参与者和报价之间的不可链接性。

5）激励的有效性

由于胜出者选择是考虑了参与者的数据效用值、参考任务价值所提理想报价等多维参数，不是只单方面考虑最低报价，并且对竞标失败者也给予一定的补偿。因此，方案做到了胜出者最优化选择，对胜出者而言奖励报酬能够满足其需求，最终对胜出者和失败者都起到较好的激励作用。

5 实验验证

为评估方案的有效性，从隐私保护度、数据精确度、时间效率和激励效果等方面进行验证。

5.1 实验数据和环境

实验过程采用仿真实验，仿真数据由群智感知系统模拟平台产生。模拟平台于三个月内陆续发布 50 个校园内不同位置的感知任务，并招募一定数量的学生参与完成，对于每一个感知任务，注册人数范围为 100~1000 人。经过 50 次任务发布、拍卖和支付，平台积累了大量的仿真数据。

实验环境为 Intel i5-7200U 2.5GHz CPU、4GB 内存、Windows 7 操作系统，算法采用 Objective-C 实现。

5.2 测评指标

1）隐私保护度

参与者的隐私泄露概率 *P_reveal* 定义为竞标隐私泄露量与需要保护的竞标隐私总量的比值，如式(12)所示。

$$P_reveal = \frac{n_reveal}{N_protect} \tag{12}$$

其中，*n_reveal* 为被泄露的竞标隐私量，*N_protect* 为需要保护的竞标隐私总量。

隐私保护度 *Privacy_Degree* 定义为：

$$Privacy_Degree = 1 - P_reveal \tag{13}$$

隐私保护度越高，对隐私数据的保护水平越强。

2）数据精确度

由于隐私保护问题，会对参与者提交的匿名身份数据、加密的报价数据的精确度有一定影响。数据精确度是指匿名数据集和原始数据集之间的差异，通常用 *SSE*(sum of squared errors)进行度量。*SSE* 表示了匿名数据集和原始数据集中所有记录的属性距离的平方和，如式(14)所示。

$$SSE = \sum_{x_i \in X} \sum_{a_i^n \in x_i} \left(dist\left(a_i^n, (a_i^n)'\right)\right)^2 \tag{14}$$

其中，a_i^n是原始数据集中第 *i* 个记录的第 *n* 个属性，$(a_i^n)'$是匿名数据集中第 *i* 个记录的第 *n* 个属性。*dist*()是距离函数。*SSE* 的值越小，数据精确度越高，数据的可用性越好。

3）时间效率

拍卖时间 T_i 定义为从开始注册到选出胜出者所经历的运行时间，如式(15)所示。

$$T_i = t_{win} - t_{reg} \quad (1 \le i \le n) \tag{15}$$

其中，t_{win} 表示选出胜出者的时刻，t_{reg} 表示开始注册的时刻，*n* 表示拍卖总次数，*i* 表示第 *i* 次拍卖。

算法时间效率用 *T(n)*来度量，*T(n)*为 *n* 次拍卖时间的平均值，如式(16)所示。*T(n)*的值越小，算法的时间效率越高。

$$T(n) = \frac{1}{n} \sum_{i=1}^{n} (T_i) \tag{16}$$

4）激励效果

用户参与率和满意度能够反映方案的激励效果。用户参与率 *P_work* 定义为参与竞标人数与注册人数的比值，如式(17)所示。

$$P_work = \frac{n_bid}{N_reg} \tag{17}$$

其中，*n_bid* 表示参与竞标人数，*N_reg* 表示注册人数。

参与感知任务的用户在完成任务并获得相应报酬后对平台做出评价，评价结果 *e* 设定两个等级，如式(18)所示。

$$e = \begin{cases} 1 & \text{满意} \\ 0 & \text{不满意} \end{cases} \tag{18}$$

用户满意度 *S* 定义为给出评价结果为“1”的用户人数与参与评价总人数的比值，如式(19)所示。

$$S = \frac{n_{(e=1)}}{N_evaluate} \tag{19}$$

其中，$n_{(e=1)}$表示给出评价结果为“1”的用户人数，*N_evaluate* 表示参与评价的总人数。

5.3 实验结果与分析

对于隐私保护度、数据精确度、时间效率的测试，在相同仿真数据和实验环境下，将本文算法与 PRIDE、TTP 两种隐私保护方案进行对比。PRIDE[13]是认知无线电网络中的一种隐私保护和频谱拍卖方案，它利用了复杂密码技术（如安全多方计算，保序加密以及不经意传输协议）以获得最低报价并保护报价隐私。TTP（Trusted Third Party）[8]是可信第三方群组机制，该机制引入一个完全可信的第三方来执行群组竞标，有关参与者的所有信息，如报价，ID 和时空矩阵，对于 TTP 都是透明的，参与者的隐私完全依赖于 TTP。

通过设置隐私阈值为[0.1~1.0]，测试得到三种算法的隐私保护度对比，如图 2 所示。

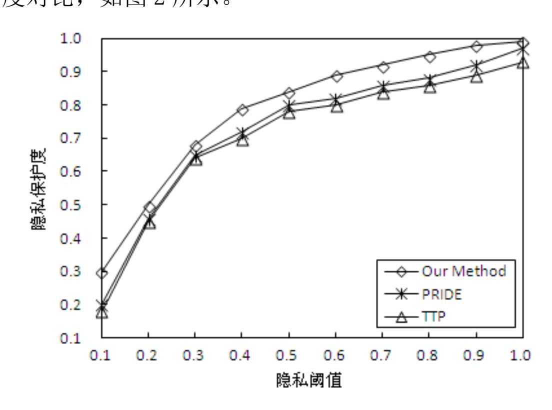


图 2 三种算法隐私保护度对比

由图 2 可知，随着隐私阈值的增大，三种算法的隐私保护度均呈上升趋势。因为隐私阈值设置的越高，算法对参与者隐私数据的保护水平越强。在相同的隐私阈值条件下，本文算法的隐私保护度比 PRIDE 和 TTP 都高。由于本文算法借助参与者的临时公钥用具有抗冲突性的安全加密哈希函数生成多于 256 位的可变地址序列来保护参与者身份，并结合随机数对候选参与节点的效用报价进行隐匿，而 PRIDE 和 TTP 算法都不具有抗冲突性和生成可变地址序列的特性，所以本文算法的隐私保护水平更强，隐私保护度优于以上两种算法。

图 3 为三种算法的数据精确度对比，同样设置隐私阈值为[0.1~1.0]。

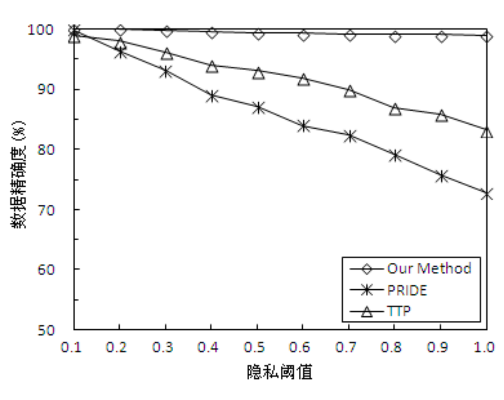


图 3 三种算法数据精确度对比

由图 3 可知，随着隐私阈值的增大，PRIDE 和 TTP 算法的数据精确度都呈下降趋势，而本文算法的数据精确度一直趋近于 100%。因为 PRIDE 算法采用复杂密码技术进行报价隐私保护，隐私阈值越大，其对报价数据加密的复杂度越高，对报价数据隐匿的程度也越高，从而导致数据的精度下降越大。TTP 算法采用可信第三方来保护参与者的所有隐私，随着隐私阈值的增大，可信第三方对参与者隐私的保护级别也越高，通过群组竞标来隐匿真实参与者身份等信息的混淆度越高，导致数据精确度下降较大。本文算法采用轻量级数据加密技术，不必进行复杂的加密运算，就能对参与者身份和报价数据进行隐私保护，数据的精确度受隐私阈值影响较小。

图 4 为三种算法的时间效率对比。

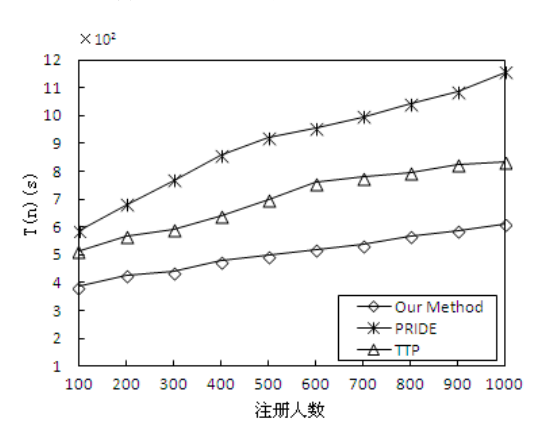


图 4 三种算法时间效率对比

由图 4 可知，随着注册人数的增加，三种算法的 $T(n)$ 都随之增大。因为算法的运行时间会随着人数规模的增大而增加。但本文算法在注册人数增加情况下 $T(n)$ 仅有小幅增加，而 PRIDE 和 TTP 算法都高于本文算法，尤其是 PRIDE 算法，$T(n)$ 增加的幅度最大。可见，在相同的测试条件下，本文算法在时间效率方面更有优势。

对于激励效果的测试，将本机制与 Lee 等人[13]提出的动态价格逆向拍卖机制 RADP、固定价格随机选择机制 RSFP 两种激励机制进行对比。RADP 和 RSFP 机制采用只对胜出者支付报酬，且都未考虑参与者隐私保护问题。用相同的仿真数据（即 50 个校园感知任务的发布、拍卖和支付），注册人数为 100~1000 人的情况下，对三种机制进行测试，得到用户参与率和用户满意度对比分别如图 5、6 所示。

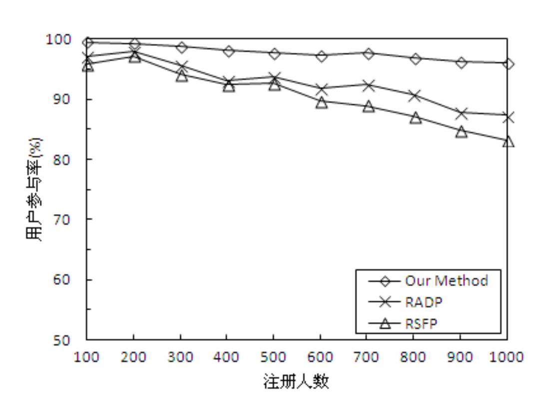


图 5 三种机制用户参与率对比

由图 5 可知，随着注册人数的增加，本机制的用户参与率一直保持在 95%以上，而 RADP 和 RSFP 两种机制均呈下降趋势，当注册人数达到 1000 人时，两者的用户参与率都降到 90%以下。因为本机制不但考虑了参与者的数据完整率和数据质量，而且是依据效用报价进行胜出者最优选择，对失败者也支付一定的报酬，同时在整个拍卖过程中对参与者身份和报价隐私进行保护。可见，本机制的用户参与率更高，说明它在激励用户参与执行感知任务方面具有更好效果。

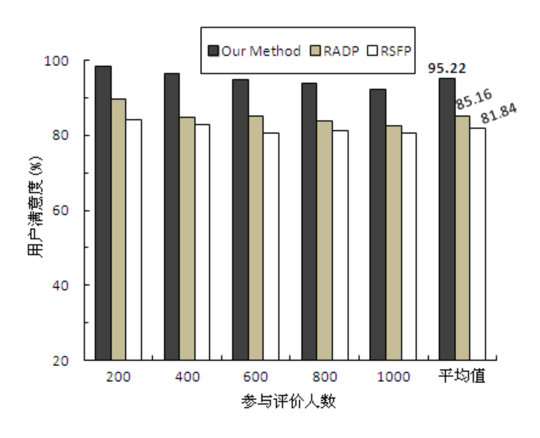


图 6 三种机制用户满意度对比

由图 6 可知，在参与评价人数分别为 200、400、600、800、1000 时，本机制的用户满意度都比 RADP 和 RSFP 高，平均满意度为 95.22%，而 RADP 的平均满意度为 85.16%，RSFP 的平均满意度为 81.84%。可见，参与者对该机制的激励方式非常肯定。

从图 2~6 所示的实验结果得出结论，该机制在隐私保护度、数据精确度、时间效率和激励效果等方面比现有激励机制更具优势，说明该机制有效。

6 结束语

本文提出一种支持隐私保护的动态激励机制，旨在解决用户隐私泄露等原因导致的群智感知激励机制效果不佳的问题。该机制利用轻量级隐私保护方法，结合数据加密技术，支持参与者匿名注册，并在竞标阶段为参与者的效用报价提供隐私保护，效用报价由参与者的数据完整率、数据质量以及理想报价等多维参数决定。最后依据效用报价对胜出者进行优选并支付，对竞标失败者也有一定补偿，以此发挥激励作用。仿真实验证明机制在隐私保护度、数据精确度、时间效率和激励效果等方

面相比同类方案均有较优表现。在后续的研究中，尝试将报酬支付环节数据的隐私保护纳入机制的保护范畴，使机制更加完善。

参考文献：

[1] Guo Bin, Chen Huihui, Yu Zhiwen, *et al.* Fliermeet: a mobile crowdsensing system for cross-space public information reposting, tagging, and sharing [J]. IEEE Trans on Mobile Computing, 2015, 14 (10): 2020-2033.

[2] Ganti R K, Ye Fan, Lei Hui. Mobile crowdsensing: Current state and future challenges [J]. IEEE Communications Magazine, 2011, 49 (11): 32-39.

[3] Wang Yu, Xu Dingbang, Li Fan. Providing location-aware location privacy protection for mobile location-based services [J]. Tsinghua Science and Technology, 2016, 21 (3): 243-259.

[4] Lee J S, Hoh B. Sell your experiences: A market mechanism based incentive for participatory sensing [C]// Proc of IEEE International Conference on Pervasive Computing and Communications. 2010: 60-68.

[5] Jaimes L G, Vergara-Laurens I, Labrador M A. A location-based incentive mechanism for participatory sensing systems with budget constraints [C]// Proc of IEEE International Conference on Pervasive Computing and Communications. 2012: 103-108.

[6] Krontiris I, Albers A. Monetary incentives in participatory sensing using multi-attributive auctions [J]. Parallel Algorithms & Applications, 2012, 27 (4): 317-336.

[7] Shi Jing, Zhang Rui, Liu Yunzhong, *et al.* PriSense: privacy-preserving data aggregation in people-centric urban sensing systems [C]// Proc of IEEE INFOCOM. 2010: 758-766.

[8] Cristofaro E D, Soriente C. Participatoty privacy: enabling privacy in participatoty sensing [J]. IEEE Network, 2013, 27 (1): 32-36.

[9] Li Xinghua, Wang Ermeng, Yang Weidong, *et al.* DALP: a demand-aware location privacy protection scheme in continuous location-based services [J]. Concurrency & Computation Practice & Experience, 2016, 28 (4): 1219-1236.

[10] Cristofaro E D, Soriente C. Extended capabilities for a privacy-enhanced participatory sensing infrastructure (PEPSI) [J]. IEEE Trans on Information Forensics and Security, 2013, 8 (12): 2021-2033.

[11] Nojoumian M, Stinson D R. Efficient sealed-bid auction protocols using verifiable secret sharing [C]// Proc of International Conference on Information Security Practice & Experience. 2014: 302-317.

[12] 南文倩，郭斌，陈荟慧，等．基于跨空间多元交互的群智感知动态激励模型 [J]．计算机学报, 2015, 38 (12): 2412-2425. (Nan Wenqian, Guo Bin, Chen Huihui, *et al.* A cross-space, multi-interaction-based dynamic incentive mechanism for mobile crowd sensing [J]. Chinese Journal of Computers, 2015, 38 (12): 2412-2425.)

[13] Wu Fan, Huang Qianyi, Tao Yixin, *et al.* Towards privacy preservation in strategy-proof spectrum auction mechanisms for noncooperative wireless networks [J]. IEEE//ACM Trans on Networking, 2015, 23 (4): 1271-1285.

[14] 沈楠，袁科，贾春福．一种增强的位置分享隐私保护方案 [J]．计算机应用研究, 2017, 34 (3): 862-866, 887. (Shen Nan, Yuan Ke, Jia Chunfu. Enhanced privacy-preserving location sharing mechanism [J]. Application Research of Computers, 2017, 34 (3): 862-866, 887.)